Exhibit: OpenAI Student Data Privacy Agreement

This Student Data Privacy Agreement ("**DPA**") is entered into by and between [Customer] ("**Customer**") and OpenAI, LLC ("**OpenAI**" and together with Customer, the "**Parties**") pursuant to the Business Terms or other agreement for OpenAI services by and between the Parties, effective as of [Effective Date of Services Agreement] (the "**Services Agreement**"). This DPA is effective as of the effective date of the Services Agreement ("**Effective Date**"). Capitalized terms shall have the meanings set forth in **Exhibit A**.

1. Background. This Student DPA describes the duties and responsibilities of each Party to protect the privacy and security of Student Data and to comply with Privacy Laws. In performing the Services, OpenAI shall be considered a School Official with a legitimate educational interest. OpenAI shall be under the direct control and supervision of Customer with respect to its use of Student Data. In order to receive the Services, Customer may provide, or OpenAI may collect on behalf of Customer, the Student Data as identified in **Exhibit B** (Schedule of Data).

2. Data Ownership and Authorized Access.

   2.1. *Student Data Property of Customer*. The Parties acknowledge and agree that (a) all Student Data transmitted to OpenAI pursuant to the Services Agreement is and will continue to be the property of and under the control of Customer; (b) all copies of such Student Data transmitted to OpenAI, including any modifications or additions or any portion thereof, are subject to the provisions of this DPA in the same manner as the original Student Data; and (c) as between them, all rights, including all intellectual property rights in and to the Student Data transmitted pursuant to the Services Agreement, shall remain the exclusive property of Customer. As a School Official, OpenAI is under the control and direction of Customer as it pertains to the use of Student Data.

   2.2. *Parent or Eligible Student Access*. To the extent required by law, Customer shall establish reasonable procedures by which a parent, legal guardian, or Eligible Student may review Education Records and/or Student Data, correct erroneous Education Records and/or Student Data, and transfer Student-Generated Content to a personal account, consistent with the functionality of OpenAI's Services. OpenAI shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an Customer to respond to a parent or student, whichever is sooner) to Customer's request to view or correct Student Data held by OpenAI. In the event that a parent of a student or other individual contacts OpenAI to review any of the Student Data accessed pursuant to the Services, OpenAI shall refer the parent or individual to Customer, who will follow the necessary and proper procedures regarding the requested information.

   2.3. *Separate Account*. If Student-Generated Content is stored or maintained by OpenAI, OpenAI shall, at the request of Customer, transfer, or provide a mechanism for Customer to transfer such Student-Generated Content to a separate account created by the student.

   2.4. *Law Enforcement Requests*. Should law enforcement or other government entities ("**Requesting Party**") contact OpenAI with a request for Student Data held by OpenAI pursuant to the Services, OpenAI shall notify Customer in advance of a disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform Customer of the request, or unless otherwise prohibited by law.

   2.5. *Subprocessors*. OpenAI shall enter into written agreements with all Subprocessors that require the Subprocessors to protect Student Data in a manner no less stringent than the terms of this DPA.

3. Duties of Customer.

3.1. *Privacy Compliance*. Customer shall comply with Privacy Laws, including providing notices or disclosures regarding the processing of Student Data and obtaining any consents, permissions, or authorizations for such processing, as required by Privacy Laws.

3.2. *Annual Notification of Rights*. If Customer has a policy of disclosing Education Records and/or Student Data under Privacy Laws, Customer shall include a specification of criteria for determining who constitutes a School Official and what constitutes a legitimate educational interest in its annual notification of rights.

3.3. *Reasonable Precautions*. Customer shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services and Student Data.

3.4. *Unauthorized Access Notification*. Customer shall notify OpenAI promptly of any known unauthorized access to Student Data. Customer will assist OpenAI in any efforts by OpenAI to investigate and respond to unauthorized access to Student Data.

3.5. *No Users Under 13*. In accordance with the Services Agreement, Customer will not send OpenAI Student Data associated with children under the age of thirteen (13).

3.6. *Product Set Up.* Customer shall review and set up accounts in accordance with OpenAI's Educational Implementation Guide, available at **Exhibit D**. Customer is responsible for reviewing each setting and ensuring the defaults align with OpenAI's instructions.

4. Duties of OpenAI.

4.1. *Privacy Compliance*. OpenAI shall comply with applicable Privacy Laws and shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data.

4.2. *Authorized Use*. The Student Data shared pursuant to the Services Agreement, including persistent unique identifiers, shall be used for no other purpose other than to provide the Services or as otherwise permitted or required by Privacy Laws or this DPA. For purposes of clarity, OpenAI may: (a) create De-Identified Data and OpenAI shall own such De-Identified Data; (b) use and disclose Student Data as part of the maintenance, development, support, operation, or improvement of OpenAI's products or services; (c) disclose Student Data in response to law enforcement requests and legal process; and (d) disclose Student Data where required by law.

4.3. *No Data Sharing*. OpenAI acknowledges and agrees that it shall not share any Student Data or any portion thereof other than as directed or permitted by Customer or this DPA. For purposes of clarity, this prohibition against sharing shall not apply to (a) De-Identified Information, (b) Student Data disclosed in response to a law enforcement request or legal process, (c) Student Data disclosed where required by law, or (d) Student Data disclosed to Subprocessors pursuant to this DPA. For additional clarity, OpenAI will not sell Student Data to any third party.

4.4. *De-Identified Data*. OpenAI will not attempt to re-identify De-Identified Data. De-Identified Data may be used by OpenAI for those purposes allowed under Privacy Laws.

4.5. *Disposition of Data*. Upon termination of this DPA, OpenAI shall dispose of all Student Data after providing Customer with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to Section 2.3.

4.6. *Advertising Limitations*. OpenAI will not engage in Targeted Advertising using Student Data or amass a profile of a student for any purpose other than providing the Services to Customer. This section does not prohibit OpenAI from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); (ii) to make product recommendations to teachers or Customer employees; or (iii) from otherwise using Student Data as permitted in the Agreement, this DPA and its accompanying exhibits.

5. Data Security.

5.1. *Data Security*. OpenAI will maintain an information security program designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. Such program shall include the minimum standards set forth on **Exhibit C** hereto.

5.2. *Security Incident*. In the event that OpenAI discovers or otherwise becomes aware of a Security Incident, OpenAI shall: (a) notify Customer without undue delay and in any event within the time required by applicable Privacy Laws; (b) provide Customer with written details of such Security Incident, including the type of data affected and the identity of any affected students, parents, or guardians, promptly after such details become known or reasonably available to OpenAI; (c) provide timely information and cooperation as Customer may reasonably request to fulfill its data breach reporting obligations under applicable laws; and (d) take such measures and actions as are reasonable to remedy or mitigate the effects of such Security Incident. In fulfilling any reporting obligations under Privacy Laws, Customer shall be responsible for providing notice to affected students, parents, or guardians.

6. Miscellaneous. This DPA and the Services Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. The delay or omission by either party to exercise any right hereunder shall not be construed as a waiver of such right. This DPA shall terminate upon the termination of the Services Agreement unless otherwise agreed in writing. The following provisions will conform with the Services Agreement: (a) Assignment, (b) Notices, and (c) Jurisdiction, Venue, and Choice of Law. In the event that any provision of this Agreement is determined to be illegal or unenforceable, that provision will be limited or eliminated so that this Agreement will otherwise remain in full force and effect and enforceable. In the event of a conflict between the terms of this DPA and any other agreement, including, but not limited to, the Services Agreement, or either Parties' Privacy Policies, the terms of this DPA will control.

IN WITNESS WHEREOF, Customer and OpenAI execute this DPA as of the Effective Date.

OpenAI, L.L.C.

Signature: Kevin Mills

Name: Kevin Mills

Title: Authorized Signer

Date: 5/21/2025

Canyons School District

Signature: Scot McCombs

Name: Scot McCombs

Title: Director of IT

Date: 5/13/25

EXHIBIT A: DEFINITIONS

De-Identified Data means records and information where all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific individual.

Education Records means records, files, documents, and other materials which contain information directly related to a student and maintained by an educational agency or institution or by a person acting for such agency or institution. For the sake of clarity, Education Records can include, but are not limited to, general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Eligible Student means a student who is 18 years or older or is attending an institution of postsecondary education.

Metadata means information that provides meaning and context to other data being collected by OpenAI. Metadata that does not include any, or that has been stripped of all, direct and indirect identifiers of a student, is considered De-Identified Data.

Privacy Laws means U.S. federal or state privacy or security laws governing the use, disclosure, or processing of Student Data, including, as applicable:

A. the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g and 34 C.F.R. Part 99 ("**FERPA**");

B. the Protection of Pupil Rights Amendment, 20 U.S.C. § 1232h ("**PPRA**"); and

C. the U.S. state laws and regulations referenced at **Exhibit E** for the state in which Customer is located.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a "School Official" is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and sharing of personally identifiable information from Education Records.

Security Incident means the unauthorized access, destruction, use, modification, disclosure, or acquisition of information that compromises the security, confidentiality, or integrity of the Student Data maintained by OpenAI.

Student-Generated Content means materials or content created by a student pursuant to the Services Agreement, including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, and videos.

Student Data means students' personally identifiable information and materials provided by Customer to OpenAI or directly collected by or on behalf of OpenAI pursuant to the Services Agreement, the categories of which are described at **Exhibit B**, and Student-Generated Content. Student Data includes Metadata and "Personally Identifiable Information" (PII), as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of OpenAI's services.

Subprocessor means a party other than Customer or OpenAI, who OpenAI engages for data collection, analytics, storage, or other service to operate and/or improve its service, and who processes Student Data.

Targeted Advertising means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the student's online behavior, usage of applications, or Student Data. "Targeted Advertising" does not include any advertising to a student on an online location based on the student's current visit to that location or in response to a student's response or request for information or feedback, if the student's online activities or requests are not retained over time for the purpose of targeting subsequent advertisements.

EXHIBIT B: SCHEDULE OF DATA

Name, contact information, demographic information, and any other information provided by the user through the Services' open input fields.

EXHIBIT C: TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

INTRODUCTION

This Exhibit describes the information security program and security standards that OpenAI maintains with respect to the Services and handling of data submitted by or on behalf of Customer of the Services (the "Customer Data"). Capitalized terms not defined in this Exhibit have the meanings given in the DPA or Agreement.

To learn more about OpenAI's technical and organizational security measures to protect Customer Data, see the OpenAI Trust Portal at https://trust.openai.com/ (the "Trust Portal"). The Security Measures below include the subset of the information available in the Trust Portal which applies to this DPA.

SECURITY MEASURES

Corporate Identity, Authentication, and Authorization Controls. OpenAI maintains industry best practices for authenticating and authorizing internal employee and service access, including the following measures:

- OpenAI uses single sign-on (SSO) to authenticate to third-party services used in the delivery of the Services. Role Based Access Controls (RBAC) are used when provisioning internal access to the Services;
- Mandatory multi-factor authentication is used for authenticating to OpenAI's identity provider.
- Unique login identifiers are assigned to each user;
- Established review and approval processes for any access requests to services storing Customer Data;
- Periodic access audits designed to ensure access levels are appropriate for the roles each user performs;
- Established procedures for promptly revoking access rights upon employee separation;
- Established procedures for reporting and revoking compromised credentials such as passwords and API keys); and
- Established password reset procedures, including procedures designed to verify the identity of a user prior to a new, replacement, or temporary password.

Customer Identity, Authentication, and Authorization Controls. OpenAI maintains industry best practices for authenticating and authorizing customers to the Services, including the following measures:

- Use of a third-party identity access management service to manage Customer identity, meaning OpenAI does not store user-provided passwords on users' behalf; and
- Logically separating Customer Data by organization account using unique identifiers. Within an organization account, unique user accounts are supported.
- Cloud Infrastructure and Network Security. OpenAI maintains industry best practices for securing and operating its cloud infrastructure, including the following measures:
- Separate production and non-production environments;
- Primary backend resources are deployed behind a VPN.
- The Services are routinely audited for security vulnerabilities.
- Application secrets and service accounts are managed by a secrets management service;
- Network security policies and firewalls are configured for least-privilege access against a pre-established set of permissible traffic flows. Non-permitted traffic flows are blocked; and
- Services logs are monitored for security and availability.

System and Workstation Control. OpenAI maintains industry best practices for securing OpenAI's corporate systems, including laptops and on-premises infrastructure, including:

- Endpoint management of corporate workstations;
- Endpoint management of mobile devices;
- Automatic application of security configurations to workstations;

- Mandatory patch management; and
- Maintaining appropriate security logs.

Data Access Control. OpenAI maintains industry best practices for preventing authorized users from accessing data beyond their authorized access rights and for preventing the unauthorized input, reading, copying, removal, modification, or disclosure of data. Such measures include the following:

- Employee access to the Services follows the principle of least privilege. Only employees whose job function involves supporting the delivery of Services are credentialed to the Services environment; and
- Customer Data submitted to the Services is only used in accordance with the terms of the DPA, Agreement, and any other applicable contractual agreements in place with Customer.

Disclosure Control. OpenAI maintains industry best practices for preventing the unauthorized access, alteration, or removal of data during transfer, and for securing and logging all transfers. Such measures include:

- Encryption of data at rest in production datastores using strong encryption algorithms;
- Encryption of data in transit;
- Audit trail for all data access requests for production datastores;
- Full-disk encryption required on all corporate workstations;
- Device management controls required on all corporate workstations;
- Restrictions on use of portable or removable media; and
- Customer Data can be deleted upon request.

Availability control. OpenAI maintains industry best practices for maintaining Services functionality through accidental or malicious intent, including:

- Ensuring that systems may be restored in the event of an interruption;
- Ensuring that systems are functioning and faults are reported; and
- Anti-malware and intrusion detection/prevention solutions implemented comprehensively across our environment.

Segregation control. OpenAI maintains industry best practices for separate processing of data collected for different purposes, including:

- Logical segregation of Customer Data;
- Restriction of access to data stored for different purposes according to staff roles and responsibilities;
- Segregation of business information system functions; and
- Segregation of testing and production information system environments.

Risk Management. OpenAI maintains industry best practices for detecting and managing cybersecurity risks, including:

- Threat modeling to document and triage sources of security risk for prioritization and remediation;
- Penetration testing is conducted on the Services at least annually, and any remediation items identified are resolved as soon as possible on a timetable commensurate with the associated risk. Upon request, OpenAI will provide summary details of the tests performed and whether the identified issues have been resolved;
- Annual engagements of a qualified, independent external auditor to conduct periodic reviews of OpenAI's security practices against recognized audit standards, including SOC 2 Type II certification audits. Upon reasonable request, OpenAI will provide summary details; and
- A vulnerability management program designed to ensure the prompt remediation of vulnerabilities affecting the Services.

Personnel. OpenAI maintains industry best practices for vetting, training, and managing personnel with respect to security matters, including:

- Background checks, where legally permissible, of employees with access to Customer Data or supporting other aspects of the Services;
- Annual security training for employees, and supplemental security training as appropriate.

Physical Access Control. OpenAI maintains industry best practices for preventing unauthorized physical access to OpenAI facilities, including:

- Physical barrier controls including locked doors and gates;
- 24-hour on-site security guard staffing;
- 24-hour video surveillance and alarm systems, including video surveillance of common areas and facility entrance and exit points;
- Access control systems requiring biometrics or photo-ID badge and PIN for entry to all OpenAI facilities by OpenAI personnel;
- Visitor identification,sign-in and escort protocols; and
- Logging of facility exits and entries.

Third Party Risk Management. OpenAI maintains industry best practices for managing third party security risks, including with respect to any subprocessor or subcontractor to whom OpenAI provides Customer Data, including the following measures:

- Written contracts designed to ensure that any agent agrees to maintain reasonable and appropriate safeguards to protect Customer Data; and
- Vendor Security Assessments: All third parties undergo a formal vendor assessment process maintained by OpenAI's Security team.

Security Incident Response. OpenAI maintains a security incident response plan for responding to and resolving events that compromise the confidentiality, availability, or integrity of the Services or Customer Data including the following:

- OpenAI aggregates system logs for security and general observability from a range of systems to facilitate detection and response; and
- If OpenAI becomes aware that a Personal Data Breach has occurred, OpenAI will notify Customer in accordance with the DPA.

Security Evaluations. OpenAI performs regular security and vulnerability testing to assess whether key controls are implemented properly and are effective as measured against industry security standards and its policies and procedures and to ensure continued compliance with obligations imposed by law, regulation, or contract with respect to the security of Customer Data as well as the maintenance and structure of OpenAI's information systems.

EXHIBIT D: EDUCATIONAL IMPLEMENTATION GUIDE

This Educational Implementation Guide is provided to assist Customers in setting the minimum product configurations required under their contract. It is also intended to help customers processing Student Data to use the Services consistent with applicable Privacy Laws and their compliance obligations. However, the information in this Guide does not constitute legal advice and adhering to this guidance does not ensure your compliance with applicable Privacy Laws. Customers are solely responsible for independently evaluating their own specific use of the Services as appropriate to support their legal compliance obligations, as the recommendations in the Guide are not exhaustive.

We may update or revise this guidance from time to time, including to provide guidance for new features or services as they are released.

General Configuration and Use Considerations

This section provides general guidance regarding certain features to consider as you configure and use the Services consistent with your compliance obligations.

1. **Access Management.** You are responsible for configuring use of single sign-on ("SSO") to manage access and authorization and for implementing other access management requirements for your End Users when accessing the Services. Please see OpenAI's help article regarding SSO for more information.
2. **Mobile Device Management**. You are responsible for securing devices that are used to access the Services in accordance with your compliance obligations. The Services do not control the encryption, geolocation, remote wiping or other security features of devices. OpenAI may store some data (such as message edits in progress) locally on a device running the OpenAI app or browser session. If your organization's policy or applicable Privacy Laws require encryption of Student Data at rest, you must encrypt all devices that run OpenAI applications or browser sessions.
3. **Monitoring.** You are responsible for implementing your own tools and processes for monitoring your End Users' use of the Services.
4. **Local Privacy Law Requirements**. You are responsible for confirming that your use of the Services is consistent with applicable local Privacy Laws.

Using ChatGPT Edu or Enterprise With Student Data

When you use ChatGPT Edu or ChatGPT Enterprise, the full capabilities of the Services are available to you by default. Prior to you or your End Users transmitting, uploading, or communicating about Student Data through the Services, it is your responsibility to configure the following settings of the Services as described below, consistent with your compliance obligations.

1. **Workspace Settings**. The "Settings" tab enables you to manage the below capabilities of your ChatGPT workspace. Please see OpenAI's help article regarding workspace settings for more information.
    a. **Sharing.** The "Chats can be shared with…" toggle under "Sharing" is a capability that allows you to control how your End Users can share their chats. You are solely responsible for evaluating and configuring these tools in accordance with your legal obligations under applicable Privacy Laws.The configurations are described below:
        i. If you set the sharing toggle to "Workspace members only," End Users are able to share their chats internally, which could result in Student Data being transmitted to any End User in your workspace. If you choose this setting, you must have made the determination that all End Users of your workspace are authorized to access any other End Users' Student Data shared over chats, and that determination should be documented in writing.
        ii. If you set these sharing toggles to "No one," End Users are not able to share their chats with others.
    b. **Connected Apps**. Enabling your End Users to connect to external apps like Google Drive and Microsoft OneDrive can involve transmitting information to third parties. If you enable this capability, you are solely responsible for implementing internal policies with respect to review and use of each app in accordance with your legal obligations under applicable Privacy Laws. Otherwise, you can choose to disable this functionality by toggling off each app under the "Connected Apps" settings.
2. **GPTs Settings**. The "GPTs" tab enables you to manage the below capabilities of your ChatGPT workspace's GPTs.

Please see OpenAI's help article regarding GPT settings for more information.

a. **Sharing.** The "GPTs can be shared with…" toggle under "Sharing" is a capability that allows you to control how your End Users can share their GPTs. You are solely responsible for evaluating and configuring these tools, as described below:

   i. Do not set the sharing toggle to "Anyone." If you set the sharing toggle to "Anyone," End Users are able to share their GPTs externally, which could result in Student Data being transmitted to third parties outside of the workspace.

   ii. If you set the sharing toggle to "Workspace members only," End Users are able to share their GPTs internally, which could result in Student Data being transmitted to any End User in your workspace. If you choose this setting, you have made the determination that all End Users of your workspace are authorized to access any other End Users' Student Data shared over GPTs., and that determination should be documented in writing.

   iii. If you set these sharing toggles to "No one," End Users are not able to share their GPTs with others.

b. **Plugins and Actions.** If enabled, the use of Plugins and/or Actions can involve transmitting Student Data to third parties. You must disable these capabilities through the "Plugins" and "Custom Actions" toggles under the "Workspace" settings.

c. **Browse.** If enabled, the use of the web browsing capabilities can result in transmitting Student Data to a third-party website. You must disable this functionality through the "Browsing with Bing" toggle under the "Workspace" settings.

d. **Third-Party GPTs.** The use of GPTs built by third parties can involve transmitting information to third parties. If you enable this capability, you are solely responsible for implementing internal policies with respect to review and use of each third-party GPT in accordance with your legal obligations under applicable Privacy Laws. Otherwise, you can choose to disable this functionality by selecting "Don't Allow" under "Third Party GPTs."

3. **Data Retention**. Unless earlier deleted by an End User or unless you have selected a shorter retention period, OpenAI will maintain your data for the duration of your agreement with OpenAI. You are responsible for removing any data that needs to be removed using self-service tools provided in the Services, such as the ability to delete chats.

EXHIBIT E: SUPPLEMENTAL STATE TERMS

Customer and OpenAI will comply with the state laws and regulations to the extent applicable to the state in which Customer receives the services, as more fully set forth in this **Exhibit E**. In the event of a conflict between the DPA and this **Exhibit E**, the more restrictive terms will control.

SUPPLEMENTAL STATE TERMS FOR CALIFORNIA. The Parties will comply, as applicable, with Cal. Educ. Code § 49073.1. ("AB 1584") and the Student Online Personal Information Protection Act at Cal. Bus. & Prof. Code § 22584 ("SOPIPA").

1. OpenAI will provide training on the security and confidentiality of Student Data to responsible individuals.

2. Customer and OpenAI agree that OpenAI will notify Customer of any Security Incident promptly after becoming aware of the incident, unless doing so would impede any law enforcement investigation.

3. Section 4.5 is amended as follows:

   Upon termination of this DPA, OpenAI shall dispose of all Student Data after providing Customer with reasonable prior notice. **Upon written request from Customer, OpenAI shall dispose of or provide a mechanism for Customer to transfer Student Data obtained under the Services Agreement within a reasonable time of said request and according to a schedule and procedure as the Parties may reasonably agree.** The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to Section 2.3.

SUPPLEMENTAL STATE TERMS FOR CONNECTICUT. The Parties will comply, as applicable, with Conn. Gen. Stat. § 10-234aa et seq.; and

1. Section 2.1 of the DPA is amended as follows:

   The Parties acknowledge and agree that (a) all Student Data transmitted to OpenAI pursuant to the Services Agreement is and will continue to be the property of and under the control of Customer; (b) all copies of such Student Data transmitted to OpenAI, including any modifications or additions or any portion thereof, are subject to the provisions of this DPA in the same manner as the original Student Data; and (c) as between them, all rights, including all intellectual property rights in and to the Student Data transmitted pursuant to the Services Agreement, shall remain the exclusive property of Customer. **All Student-Generated Content shall be the property of the student or the parent or legal guardian of the student**. As a School Official, OpenAI is under the control and direction of Customer as it pertains to the use of Student Data.

2. Customer and OpenAI agree that OpenAI will notify the local or regional board of education of any Security Incident that results in the unauthorized release, disclosure or acquisition of Student Data within thirty (30) days after the discovery of the incident, unless doing so would impede any law enforcement investigation.

   The contact information for the local or regional board of education is:

   Phone: _____ Email: _____

3. Customer and OpenAI agree that OpenAI is responsible for notifying the parent, legal guardian, or eligible student of any Security Incident that results in the unauthorized release, disclosure or acquisition of Student Data or Student-Generated Content within thirty (30) days after the discovery of said Security Incident.

4. Section 4.5 is amended as follows:

   Upon termination of this DPA, OpenAI shall dispose of all Student Data after providing Customer with reasonable prior notice. **Upon written request from Customer, OpenAI shall dispose of or provide a mechanism for Customer to transfer Student Data obtained under the Services Agreement within a reasonable time of said request and according to a schedule and procedure as the Parties may reasonably agree, unless (A) state or federal law prohibit such deletion or require retention, or (B) a copy of such Student Data is part of a disaster recovery storage system and is inaccessible to the public and unable to be used in the normal course of business, provided that a deletion request can be made if such copy is used by OpenAI to repopulate accessible data following a disaster recovery.** The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to Section 2.3.

5. OpenAI shall implement and maintain reasonable security procedures and practices designed to protect Student Data from unauthorized access, destruction, use, modification or disclosure that, based on the sensitivity of the Student Data and risk from unauthorized access:

    a. Use technologies and methodologies that are consistent with guidance issued pursuant to Section 13402(h)(2) of Public Law 111-5, as amended from time to time;

    b. Maintain technical safeguards for Student Data in a manner consistent with the provisions of 45 CFR 164.312, as amended from time to time; and

    c. Otherwise meet or exceed industry standards.

6. The laws of Connecticut shall govern the rights and duties of OpenAI and Customer.

SUPPLEMENTAL STATE TERMS FOR GEORGIA. The Parties will comply, as applicable, with the Student Data Privacy, Accessibility, and Transparency Act at O.C.G.A. § 20-2-660 et seq.

1. Section 4.5 is amended as follows:

    Upon termination of this DPA, OpenAI shall dispose of all Student Data after providing Customer with reasonable prior notice. **Upon written request from Customer, OpenAI shall dispose of or provide a mechanism for Customer to transfer Student Data obtained under the Services Agreement within forty-five (45) days of said request and according to a schedule and procedure as the Parties may reasonably agree.** The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to Section 2.3.

SUPPLEMENTAL STATE TERMS FOR KANSAS. The Parties will comply, as applicable, with Kan. Stat. §§ 72-6312 et seq and Kan. Stat. §§ 72-6331 et seq.

1. Section 4.5 is amended as follows:

    Upon termination of this DPA, OpenAI shall dispose of all Student Data after providing Customer with reasonable prior notice. **Upon written request from Customer, OpenAI shall dispose of or provide a mechanism for Customer to transfer Student Data obtained under the Services Agreement within a reasonable time of said request and according to a schedule and procedure as the Parties may reasonably agree, unless the student or the student's parent or legal guardian requests that such information continue to be maintained.** The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to Section 2.3.

2. Any request by Customer for the disposition of data via destruction or deletion will comply with the NIST SP800-88 standards of data destruction.

SUPPLEMENTAL STATE TERMS FOR MAINE. The Parties will comply, as applicable, with 20-A M.R.S. §§ 6001 and Maine Student Information Privacy Act at 20-A M.R.S. § 951 et. seq. ("MSIPA").

1. Section 4.5 is amended as follows:

    Upon termination of this DPA, OpenAI shall dispose of all Student Data after providing Customer with reasonable prior notice. **Upon written request from Customer, OpenAI shall dispose of or provide a mechanism for Customer to transfer Student Data obtained under the Services Agreement within forty-five (45) days of said request and according to a schedule and procedure as the Parties may reasonably agree.** The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to Section 2.3.

SUPPLEMENTAL STATE TERMS FOR MASSACHUSETTS. The Parties will comply, as applicable, with Massachusetts General Laws, Chapter 71 §§ 34D-34H and 603 C.M.R. 23.00.

1. The Parties agree that OpenAI is considered an Authorized School Personnel for the purposes of 603 C.M.R. 23.00.

SUPPLEMENTAL STATE TERMS FOR NEW YORK. The Parties will comply, as applicable, with N.Y. Educ. Law § 2-d and 8 CRR-NY § 121.

1. OpenAI's data security and privacy plan, attached to or described in **Exhibit C**, must specify the administrative, operational, and technical safeguards in place to protect Student Data. OpenAI's plan must include a provision regarding the use of encryption technology to protect data while in motion or at rest.

2. OpenAI will limit internal access to education records to those employees that are determined to have legitimate educational interests.

3. OpenAI will provide training on Privacy Laws to all employees who have access to Student Data.

4. Customer will provide supplemental information to parents regarding OpenAI pursuant to 8 CRR-NY § 121.3. To the extent Customer requires additional information from OpenAI in order to satisfy its obligations, OpenAI will provide the information necessary prior to Student Data being shared.

5. OpenAI must notify Customer of any Security Incident without unreasonable delay but no more than seven (7) calendar days after becoming aware of said Security Incident. Customer, in turn, shall be responsible for any required reporting to the Chief Privacy Officer, as appointed pursuant to Education Law § 2-d. This shall not limit OpenAI's ability to comply with any required reporting obligations.

6. OpenAI will provide Customer details regarding where Student Data is stored in order for Customer to fulfill reporting obligations.

SUPPLEMENTAL STATE TERMS FOR PENNSYLVANIA. The Parties will comply, as applicable, with 22 Pa. Code § 12.31 and any implementing regulations and policies governing Student Data.

1. In accordance with the Pennsylvania Department of Education Data Access Policy (last revised November 2017), Customer agrees that OpenAI is acting as a School Official and represents that Customer has obtained the approval of the chief school administrator or designee to enter into this agreement.

SUPPLEMENTAL STATE TERMS FOR TEXAS. The Parties will comply, as applicable, with Tex. Educ. Code § 32.151-157, Tex. Educ. Code § 11.175, and Tex. Govt. Code § 552.114.

1. In the event of a Security Incident that constitutes a "breach of system security," as defined by Tex. Educ. Code § 11.175, Customer's designated cybersecurity coordinator, as appointed by the superintendent of the school district, shall be responsible for any required notifications on behalf of Customer. This shall not limit OpenAI's ability to comply with its own reporting obligations.

2. Section 4.5 is amended as follows:

Upon termination of this DPA, OpenAI shall dispose of all Student Data after providing Customer with reasonable prior notice. **Upon written request from Customer, OpenAI shall dispose of or provide a mechanism for Customer to transfer Student Data obtained under the Services Agreement within sixty (60) days of said request and according to a schedule and procedure as the Parties may reasonably agree.** The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to Section 2.3.

Electronic Record of Contracts

This document was generated as a record of certain contracts created, accepted and stored electronically.

Summary of Contracts

This document contains the following contracts.

Title	ID
Data Processing Agreement (Canyons School District and OpenAI)	82312703-142c-463f-90b5-fe5d8eb0f5a2

Contract signed by:

Kevin Mills

Signer ID: a3f57e71-4288-4005-96da-f927fb3d3783
Email: kmills@openai.com

Date / Time: May 21, 2025 at 2:35 AM EDT
IP Address: 212.114.212.82
User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36